Notice of data security event

The Executive Council of Physical Therapy and Occupational Therapy Examiners (ECPTOTE) recently experienced a limited data breach, and steps have been taken to address the situation promptly and mitigate potential risks.

What Happened?

On June 28, 2023, the Health Professions Council (HPC), which provides IT support to our organization and several other regulatory agencies, was notified by the Department of Information Resources (DIR) of a breach affecting the Behavioral Health Executive Council (BHEC). This breach was discovered through information posted by a known hacker group, SiegedSec. While investigating the unauthorized access to the BHEC database, HPC realized that the breached data actually pertained to ECPTOTE rather than BHEC.

HPC immediately initiated an internal investigation to assess the scope and extent of the incident. Through this investigation, it was determined that the breach primarily impacted a log file that resulted from a diagnostic script remaining from our transition from the old on-site website to the current cloud-based website. We want to emphasize that HPC has not identified any evidence of data misuse.

What Personal Information Was Involved?

The names and dates of birth of those who completed the following between June 30, 2022, and December 22, 2022, may have been accessed.

- OT and OTA licensees who completed the Jurisprudence Examination (JP Exam) after completing the CE Submission Form during the online renewal process
- PT and PTA licensees who answered the attestation questions after completing the CC Activity Summary during the online renewal process

Steps Taken to Address the Incident:

1. **Isolation and containment:** Upon detecting the breach, HPC immediately isolated the affected systems to prevent further unauthorized access. They have also implemented enhanced security measures to strengthen our overall infrastructure.
2. **Internal review and risk assessment:** In collaboration with our web hosting company and the Cybersecurity Analysts at DIR's Network Security Operations Center, HPC conducted a thorough review to identify vulnerabilities that led to the breach. The potential risks associated with the compromised data have been assessed and measures to address them have been implemented.
3. **Enhanced security measures:** Additional security protocols to reinforce our systems against future breaches have already been implemented.

4. **Collaboration with law enforcement and regulatory bodies:** The incident has been reported to the Office of the Attorney General and the Department of Information Resources, as required. We are fully cooperating with their investigations and adhering to all necessary legal and regulatory procedures.
5. **Continuous monitoring and improvement:** We are dedicated to continuous monitoring of our systems for potential vulnerabilities or threats. To ensure the ongoing effectiveness of our security measures, HPC will conduct additional audits, penetration testing, and security assessments through our web host.
6. **Notifying affected individuals:** As part of our commitment to transparency, we are in the process of emailing information similar to that contained in this document to individuals whose personal data may have been exposed in this incident. We anticipate that this will be completed by the close of business day on July 12, 2023. We are also in the process of mailing similar information to the small percentage of individuals whom we could not contact by email.

We sincerely apologize for any inconvenience or concern this incident may have caused. Protecting your personal information remains one of our top priorities, and we are committed to maintaining the trust you have placed in us.